BY ORDER OF THE COMMANDER
AIR FORCE RESERVE COMMAND

AIR FORCE RESERVE COMMAND
INSTRUCTION 33-203

1 May 1999

Communications and Information

IMPLEMENTING AFRC WIRELESS LOCAL AREA NETWORKS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AFRC WWW site at http://www.afrc.af.mil. and the AFRCEPL (CD-ROM), published monthly.

OPR: HQ AFRC/SCPI (Ms Lisa Woodson)

Certified by: HQ AFRC/SC (Col Martha Maurer)
Pages: 3
Distribution: F

This instruction implements AFRCPD 33-2, *AFRC Wireless Local Area Network*. It establishes AFRC guidance and responsibilities for implementing wireless networks in AFRC. It applies to all new and existing wireless networks used in all functions and levels of command throughout the Air Force Reserve.

1. References:

1.1. Department of Defense Joint Technical Architecture.

1.2. Air Force Technical Reference Codes.

1.3. AFI 33-103, *Requirements Development and Processing*.

1.4. AFI 33-118, *Radio Frequency Spectrum Management.*

1.5. AFSSI 4100, *The Air Force Communications Security (COMSEC) Program.*

1.6. AFSSI 5024 Vol I, *The Certification and Accreditation (C&A) Process.*

1.7. AFSSM 7011, *Emission Security Countermeasures Reviews.*

2. Responsibilities:

2.1. AFRC organizations desiring to implement a new wireless solution:

2.1.1. Identify the requirement according to AFI 33-103.

2.1.2. Provide additional information as needed to their local SC and base STEM-B to determine whether the requirement justifies a wireless solution.

2.1.3. If a wireless network solution is validated, ensure issues in paragraph **3.3.** are resolved prior to implementation of that solution.

2.1.4. Inform installation commander/designated approving authority (DAA) of any new wireless system, as he or she is responsible for ensuring Emission Security policies and standards are met.
2.1.5. Ensure DAA approval before placing wireless network into operation.

2.2. AFRC organizations with an existing wireless solution:

2.2.1. Ensure all issues in paragraph **3.3.** have been resolved.

2.2.2. Ensure installation commander/DAA is aware of the wireless system.

2.2.3. Discontinue use of any wireless network that has not been granted DAA approval to operate.

2.3. The AFRC base or wing communications and information community, or equivalent:

2.3.1. Evaluates identified network requirements to determine appropriateness of a wireless solution.

2.3.2. Ensures requirements are properly processed according to AFI 33-103.

2.3.3. Assists organizations in resolving the issues in paragraph **3.3.**

2.4. The HQ AFRC Communications and Information Directorate (SC) provides assistance and guidance as necessary.

2.4.1. HQ AFRC/SCMB:

2.4.1.1. Provides assistance and guidance on frequency management issues.

2.4.1.2. Processes frequency requests.

2.4.2. HQ AFRC/SCMD provides assistance and guidance on encryption, security, and certification and accreditation issues.

2.4.3. HQ AFRC/SCPP provides assistance and guidance on requirements processing issues.

2.4.4. HQ AFRC/SCI provides assistance and guidance on networking issues.

2.5. The base STEM-B:

2.5.1. Provides technical advice and assistance, as required, on wireless issues.

2.5.2. Documents all wireless networks in the Base C4 Systems Blueprint.

3. Procedures:

3.1. AFRC organizations that feel they have a valid need for a wireless solution should properly identify their requirement. Since wireless networking requirements are subject to the same cost thresholds and approval authority as other communications and information requirements, they must be identified and processed according to AFI 33-103.

3.2. The AFRC base or wing communications and information community (or equivalent) ensures the requirement is properly processed, including working with the STEM-B and the requesting organization to determine whether the requirement meets one of the conditions identified in AFRCPD 33-2.

3.3. If a wireless solution is justified, the following issues must be considered and resolved before that solution can be implemented:

3.3.1. All wireless networking acquisitions must meet applicable DoD and AF technical standards. Because this is a relatively new area, many of these standards are still emerging and maturing. At a minimum, wireless solutions must adhere to IEEE 802.11 (the wireless Local Area Network (LAN) standard identified in DoD Joint Technical Architecture, Vol 2, Section 2.3.3.2) and AF Technical Reference Code C4.1.1 (which identifies the mandatory features of wireless network interfaces, and also provides the desired interoperability and compliance capabilities).

3.3.2. Many commercial-off-the-shelf (COTS) wireless LAN components fall under FCC Part 15 regulations and therefore do not require governmental requests for frequency licensing. However, organizations should be aware that Part 15 devices operate in a non-licensed environment in which all have equal access to the airwaves. As a result, wireless LANs may be vulnerable to interference from other Part 15 devices (including many consumer electronic devices such as cordless phones, radio control cars, garage door openers, and baby monitors). All wireless LAN components that are not Part 15 devices require verification of proper frequency availability prior to procurement. Requests should be processed through the Command Frequency Management Office according to AFI 33-118.

3.3.3. Wireless LANs approved for use in a CONUS fixed base environment are not authorized for deployment since our federal frequency allocations and regulations are not recognized by other nations. Deployment of a wireless LAN system requires separate host nation approval and frequency allocation.

3.3.4. Like all information systems/networks, wireless LANs must be evaluated according to the Air Force Certification and Accreditation process and granted DAA approval prior to being placed into operation.

3.3.5. Because of the vulnerability of wireless LANs to interception and interpretation of data, as well as unauthorized network access, all wireless network traffic must be encrypted according to AFSSI 4100 and AFSSM 7011. Wireless LANs used for unclassified and sensitive information processing must use National Security Agency (NSA)/National Institute of Standards and Technology (NIST)-approved Type II cryptographic products, while wireless LANs used for classified processing must use NSA-approved Type I cryptographic products. Definition of Types I and II can be found in AFSSI 4100. Lack of proper encryption will result in denial of certification and accreditation and the wireless LAN cannot be used.

JAMES E. SHERRARD III, Maj Gen, USAF
Commander